



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/629,292	07/29/2003	Mihai Christodorescu	1512.149	6450
72088	7590	09/27/2007	EXAMINER	
WISCONSIN ALUMNI RESEARCH FOUNDATION C/O BOYLE FREDRICKSON S.C 840 North Plankinton Avenue Milwaukee, WI 53203			GELAGAY, SHEWAYE	
			ART UNIT	PAPER NUMBER
			2137	
			NOTIFICATION DATE DELIVERY MODE	
			09/27/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@boylefred.com

Office Action Summary	Application No.	Applicant(s)
	10/629,292	CHRISTODORESCU ET AL.
	Examiner Shewaye Gelagay	Art Unit 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 7/29/03.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-17 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-17 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 30 September 2003 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____
 5) Notice of Informal Patent Application
 6) Other: _____

DETAILED ACTION

1. Claims 1-17 have been examined.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: The specification on page 12 paragraph 56 refers to Fig.1 by discussing standardized version 31, detector 50, arrow 44 and arrow 46, however, Fig. 1 does not include standardized version 31, detector 50, arrow 44 and arrow 46. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 1-17 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-17 recite "a computer program" It is not tangibly embodied as it is only software per se. The claims should be amended to specify that "a computer program stored on a computer readable storage medium".

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-3 and 6-10 are rejected under 35 U.S.C. 102(b) as being anticipated by Nachenberg U.S. Patent Number 6,357,008.

Nachenberg teaches a computer program for identifying malicious portions in a suspect computer program comprising:

a preprocessor portion for receiving the suspect computer program and creating a logically equivalent standardized version of the suspect program; (col. 5, lines 27-39; col. 6, line 53-col. 7, line 22)

a library of standardized malicious code portions; (col. 7, line 23-col. 8, line 31; col. 9, lines 26-65) and

a detector portion reviewing the standardized version against the library of malicious code portions to provide an output indicating when a malicious code portion is

Art Unit: 2137

present in the suspect program. (col. 9, line 66-col. 10, line 10; col. 15, line 38-col. Col. 16, line 63)

As per claim 2:

Nachenberg further teaches wherein the standardized version identifies the execution order of instructions of the suspect program and wherein the detector portion reviews the instructions of the standardized version according to the execution order. (col. 2, line 38-col. 4, line 65; col. 7, line 23-col. 8, line 31; col. 9, line 26- col. 10, line 10; col. 15, line 38-col. Col. 16, line 63)

As per claim 3:

Nachenberg further teaches wherein the preprocessor identifies the execution order of the instructions by generation of a control-flow listing of the instructions. (col. 2, line 38-col. 4, line 65; col. 9, lines 26-67)

As per claim 6:

Nachenberg further teaches wherein the standardized version removes irrelevant portions of the suspect program. (col. 13, line 42-col. 15, line 37)

As per claim 7:

Nachenberg further teaches wherein the preprocessor removes irrelevant portions by identifying irrelevant portions to the detector so that the detector ignores identified irrelevant portions when reviewing the standardized version. (col. 13, line 42-col. 15, line 37)

As per claim 8:

Nachenberg further teaches wherein the irrelevant portions are one or more nop instructions. (col. 13, line 42-col. 15, line 37)

As per claim 9:

Nachenberg further teaches wherein the standardized version uses uninterpreted variables. (col. 13, line 42-col. 15, line 37)

As per claim 10:

Nachenberg further teaches wherein the suspect program is a binary executable and wherein the preprocessor receives the binary executable to generate a listing of instructions and data values. (col. 13, line 42-col. 15, line 37)

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 4-5 and 11-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg U.S. Patent Number 6,357,008 in view of Ho et al. (hereinafter Ho) U.S. Patent Number 7,188,369.

As per claims 4 and 14:

Nachenberg teaches all the subject matter as discussed above. Nachenberg does not explicitly disclose wherein the standardized version maps instructions of the suspect program to corresponding standard synonym instructions. Ho in analogous art,

however, discloses wherein the standardized version maps instructions of the suspect program to corresponding standard synonym instructions. (col. 5, lines 25-col. 6, line 40) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Nachenberg with Ho in order to receive external instructions and for execution and perform their respective antivirus functionalities. (col. 6, lines 18-21; Ho)

As per claims 5 and 15:

The combination of Nachenberg and Ho teaches all the subject matter as discussed above. In addition, Ho further teaches wherein the standard synonym instructions are different in number from the instructions of the suspect program to which the synonym instructions map. (col. 5, lines 25-col. 6, line 40)

As per claims 11 and 16:

Nachenberg teaches all the subject matter as discussed above. Nachenberg does not explicitly disclose including a library of patterns matching to one or more instructions of the suspect program and wherein the preprocessor creates the standardized version by replacing instructions of the suspect program with matching ones of the library of patterns and wherein the library of standardized malicious code portions are also collections of ones of the library of patterns. (col. 5, lines 25-col. 6, line 40) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Nachenberg with Ho in order to receive external instructions and for execution and perform their respective antivirus functionalities. (col. 6, lines 18-21; Ho)

Art Unit: 2137

As per claims 12 and 17:

The combination of Nachenberg and Ho teaches all the subject matter as discussed above. In addition, Ho further teaches wherein a pattern is at least one instruction logically replacing at least one different instruction in the suspect program. (col. 5, lines 25-col. 6, line 40)

As per claim 13:

The combination of Nachenberg and Ho teaches all the subject matter as discussed above. In addition, Ho further teaches wherein a pattern in a tag replacing at least one instruction logically having no substantive effect on the execution of the suspect program; a library of patterns is implemented as a look-up table matching instructions to the patterns. (col. 5, lines 25-col. 6, line 40)

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shewaye Gelagay 


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER